Cyber Security Staffing and Organization Strategy for the Digital Age:

The 6 Things You Need to Know

Bob Smock
Vice President, Security and Risk Management Consulting
24 May 2018

Gartner®

Texas DIR Information Security Forum

Agenda

- The Cyber Security Staffing Challenge
- Effective Cyber Security Staffing Point of View
- 6 Steps to an Effective Cyber Security Staffing Strategy
- Summary & Q&A
- Additional References

Gartner

The Challenge by the Numbers

"The main problem of obtaining key talent in the realm of cyber security stems from a lack of qualified applicants."

- The number of unfilled cybersecurity positions is expected to reach 3.5 million globally by 2021—up from one million in 2016
- It takes an average of 130 days to fill open Security positions – and Public Sector security groups are typically understaffed from 5% - 75%
- The percentage of staff with less than five years of experience increased by seven points just between 2016 and 2017
- [1]An analysis from the U.S. Bureau of Labor Statistics showed that there were 209,000 cybersecurity-related jobs that were unfilled in the U.S. during 2015 — *indicating a negative unemployment rate for cybersecurity professionals*…
- [1]In addition, the demand for security professionals will increase 53% through 2018
- Private sector/commercial organizations expect to pay cyber security salaries that are 50% - 150% above average Public Sector salaries for similar roles…
- …and include a wider array of benefits including paid professional training/certification and higher education; working hour and remote-work flexibility; extended paid time off; enhanced health benefits; on-site "stress-relief" facilities and functions; and advanced technical tools

[1] *ISACA. "State of Cyber Security 2017: Current Trends in Workforce Development", February 2017*

The unemployment rate for cybersecurity specialists is effectively zero

Gartner

Root Causes

Collectively, these forces drive Security to do more with existing staff while planning for shifting talent needs in the future

- Many of the experienced “baby boomers” with deep technical security understanding are approaching retirement age, resulting in not only a shortage of skilled workers, but also a “corporate knowledge” gap
- Organizations struggle to retain effective and high-performing security staff, resulting in a vicious cycle of high turnover and slow hiring
- The demand for security expertise in the enterprise is growing rapidly, forcing security functions to exponentially scale availability and capacity
- Factors driving this demand include incrementally larger breaches in the news, massive investments protection and transformation, and widespread adoption of agile methodologies
- Digitalization exacerbates the global shortage of security talent

A recent Gartner study identified the following critical security trends:

- Cybercrime will continue to increase due to the economic landscape
- Digital business and technology innovation will continue to challenge existing security approaches for the foreseeable future
- The higher percentage of senior, less cyber-savvy citizens are more likely to victimized by cybercriminals and related fraud
- The historical lack of investment and emphasis on protection versus compliance continues to constrain security maturity
- The decreased availability of security skillsets and increasing wage rates have resulted in a negative security-specific unemployment rate

It quickly becomes obvious that hiring more staff doesn’t remain viable for long, and the solution requires a shift on what comprises an effective workforce

Gartner

Addition to the New Normal

Digitalization exacerbates the global shortage of security talent

Digitalization requires a wider range of security roles that entail new skills and knowledge

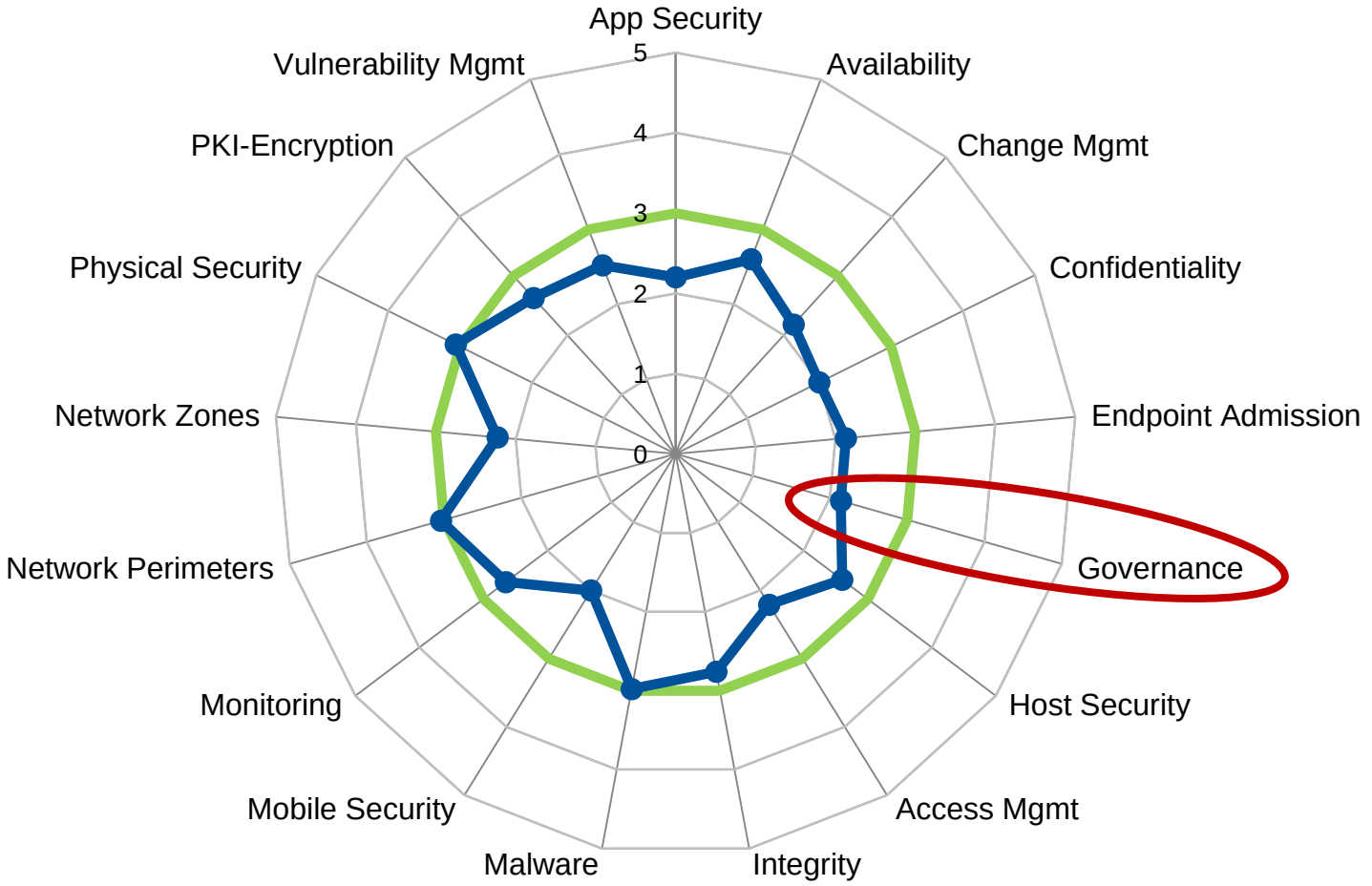
Role	Description
Sales Support	Explain the company's security efforts to external customers, build and modify controls in response to external customers, and otherwise support the sales process.
Customer Understanding	Research and conduct focus groups with external customers to identify and improve security features.
OT Security Specialist	Design and maintain security for operational technology and supporting technology.
Counterespionage Analyst	Identify, confuse, or impede attackers through activities such as creating honeypots and tarpits, disseminating misinformation, coordinating with law enforcement for takedowns, and reverse-engineering malware.
Security Service Manager	Manage and oversee the end-to-end delivery of security services to the business.
Metric Coordinator	Gather, aggregate, and report security metrics to support other security staff, function management, and external reporting needs.
Security Strategist	Set the security strategy and inform company strategy by considering the entire ecosystem of data, IT systems, regulations, security practices, cyber threats, and business trends.

Enabling digital transformation along with the "new-normal" in cyber security requires significant changes in almost all aspects of talent management including planning, recruiting, and development

Gartner

Practical Impact of the Challenge

- Public Sector aggregate cyber security maturity continues in a *Reactive* posture
- Improvements in cyber security maturity continue to be limited by *weak security governance*
- The #1 contributor to weak security governance is the lack of qualified, skilled, experienced cyber security professionals *in sufficient numbers to do what needs to be done*



The measurement of security maturity goes beyond simply existence of a control. It also includes the aspects of completeness, comprehensiveness, effectiveness, and efficiency

Gartner

Current Trends

Business leaders have a growing understanding of the significant impact of security on an organization's ability to achieve business goals, protect reputation, defend from the inevitable, and return to full functionality

Trending internal security workforce development strategies

1. Developing more virtual roles (such as virtual CISOs or privacy officers)
2. Outsourcing more operational functions to Managed Security Services Providers (MSSP)
3. Favoring cloud delivery products to reduce the maintenance overhead and remain current
4. Increasing the level of automated operational functions
5. Collaborating with universities, the military and other communities to attract emerging workers
6. Implementing an inclusive workplace culture and recruitment practices to attract a more diverse talent pool
7. Using lean security organization principles to drive security responsibilities more into the business and elsewhere in IT

Savvy security leaders are <u>not</u> exploiting this new board-level attention to simply go shopping for new security products, but instead are using this attention to gain executive-level sponsorship for new strategies to address the security skills shortage at all levels

Gartner

Addressing the Challenge

6 Things You Must Know…or at least consider.

1. Building “unicorn” teams (not unicorn people)
2. Fulfilling security talent needs through alternative approaches to hiring
3. Owning talent management rather than overly relying on the HR function
4. The lean security organization
5. Machine-learning and the hope/hype of AI
6. Changing the paradigm on security resource expectations

RACI for Security Strategy Planning

	Define Context	Define Future State	Assess Current State	Gap Analysis	Derive Roadmap	Review Strategy	Approve Strategy
Enterprise Architecture	AR	AC	I	AR	AR	A	A
Security Governance	C	R	I	C	C	C	C
Security Operations	I	I	R	C	I	I	I
Privacy	C	C	C	I	I	C	C
Digital Security Strategy Planning Committee	R	R	I	I	I	R	C
Enterprise Digital Security Coordination Committee	C	I	I	I	I	I	R

R = Responsible: Person or function that is responsible for executing the activity
A = Accountable: Person or function that owns the activity, approves work and is held accountable for it
C = Consulted: Person or function that has information relevant to the activity
I = Informed: Person or function to be informed of progress and results

ID: 340376

Prioritize building a portfolio of skills required to accomplish the mission over hiring a portfolio of traditional Security roles

Gartner

1

The Problem with Unicorns

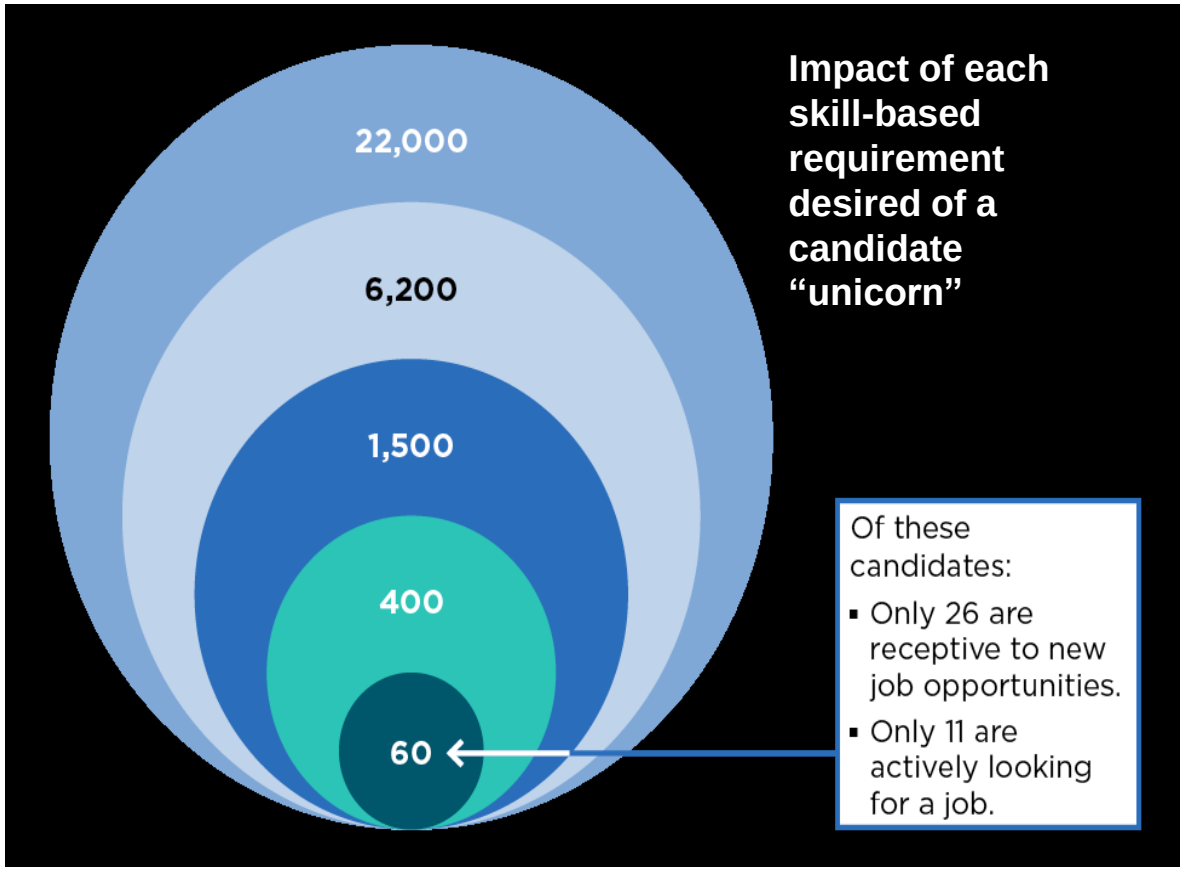
Building "unicorn" teams (not unicorn people) requires deconstructing activities fulfilled by "roles" to identify required skills

The role-based approach poses three challenges

1. Hiring for existing roles may overlook the need for new or emerging security skills
2. Traditionally defined security roles are difficult to fill because talent demand exceeds supply
3. It leads to the pursuit of "unicorn" people — individuals with an ideal combination of skills

And results in

- The search for these unicorn people focuses security on talent that is hard to find, hire, and retain
- Such an approach is largely unrealistic in today's market



Unicorn Teams *— individuals that together create a group with every desired requirement—created by identifying a complete set of security skills and competencies the Security function needs and expanding the talent pool from which Security recruits*

Gartner

Deconstructing the Unicorn

Many organizations do not have long-standing, defined organizational knowledge of security because of a legacy over-reliance on compliance vs. risk management

- **Competency**: The mix of knowledge, skills, and abilities required to deliver a desired objective
- **Knowledge:** An individual's familiarity with information, facts, or descriptions acquired through experience or education
- **Skill:** An individual's proficiency at performing a learned activity
- **Ability:** An individual's innate proficiency at and potential to perform a specific behavior at a higher proficiency

Skills and Competencies Shared Across Activities	Security Architecture and Design					Business Interfacing and Consulting					Security Operat			
	Proficiency Level Required					Proficiency Level Required					Proficiency Lev Required			
	Lowest				Highest	Lowest				Highest	Lowest			Hi
	1	2	3	4	5	1	2	3	4	5	1	2	3	4
Communication														
Presentation skills														
Internal stakeholder orientation														
Active listening and group participation														
Leadership														
Trust/integrity														
Coaching experience														
Project management experience														
Strategic thinking/visioning abilities														
Analytics														
Data analysis and modeling skills														
Statistical skills														
Creative/innovative thinking														
Insight-generation ability														
Problem Solving														
Drives enterprise-level insight and decisions														
Data visualization														
Intellectual curiosity														

Conducted as a formal exercise, deconstruct current and emerging security activities fulfilled by defined roles into a set of required skills, competencies, knowledge, and abilities

Gartner

2

Alternatives to Staff Expansion

5 indirect approaches to meeting talent needs without hiring

1. Create administrative roles that make existing technical staff more productive
2. Devolve work tasks outside of security
3. Use automation to handle repetitive, low-complexity tasks
4. Outsource for high-demand activities and skill gaps
5. Use internal talent-sharing to access new skills and expertise

1. Offload nonessential, administrative work from key security staff such as metrics, status, and presentation building
2. Over time, security often accumulates responsibilities outside of core mandates or that overlap with the broader IT function
3. Firewall monitoring, spam filtering, event logging; and offering security frameworks/APIs, code libraries, and other forms of self-service that embed security into developer workflows
4. Use to: Quickly fill labor and skills gaps not currently in-place; upskill and train existing in-house talent; fill immediate needs while focusing recruitment on emerging needs; handle commoditized activities to allow in-house talent focus on core-capabilities or highly specialized tasks
5. Opportunities to share talent between functions (e.g., IT, Legal, Internal Audit, Privacy) in ways that benefit all participants – opportunities that advance Security goals, scale benefits across the whole security function, and inject security into other risk management functions

Organizations often cite recruiting challenges as the primary cause for persistent talent gaps within the security function, but recruiting external talent is not always the best solution

Gartner

3

Owning Talent Management

Security talent management Is Security's job, not HR's

- HR should be viewed as a valuable source of information for frameworks (e.g., competency models), templates (e.g., job descriptions), and expertise (e.g., EVP statement)
- However, HR can inadvertently reduce Security talent management effectiveness
  - Where HR may not fully understand the current security talent environment
  - Many HR functions have misconceptions on security talent that actually harm or delay recruiting efforts.

HR Misconception	Reality
Certifications are required for many security roles and are useful criteria for filtering applicants.	Security certifications do not strongly correlate to actual staff performance; overlooking candidates without certifications unnecessarily reduces the talent pool.
Compensation ranges for Security roles can be based on ranges used for generalist IT roles.	Security professionals often command higher salaries than IT generalists due to the short supply and high demand for security talent.
Job listings for common Security roles are standardized and can be reused without any changes.	Leading CISOs build unicorn teams with staff that have complementary skill sets; Security recruits for different skills as the need arises—even within common roles.
Security talent is best recruited from traditional sources (e.g., large job fairs, online job markets, major universities).	Most organizations compete for the same talent; Security should look in nontraditional places to expand the talent pool.
Security job listings should focus primarily on technical skills.	Four competencies—business results orientation, decision making, influence, and organizational awareness—are the strongest predictors of Security staff performance.
Security applicants are most interested in compensation and the role's technical requirements.	Security applicants are receptive to employee value propositions that highlight the comparable benefits of working at the organization beyond compensation.

Own talent decisions from start to finish because Security is best situated to identify and understand its own talent needs

Gartner

4

The Lean Approach to Security

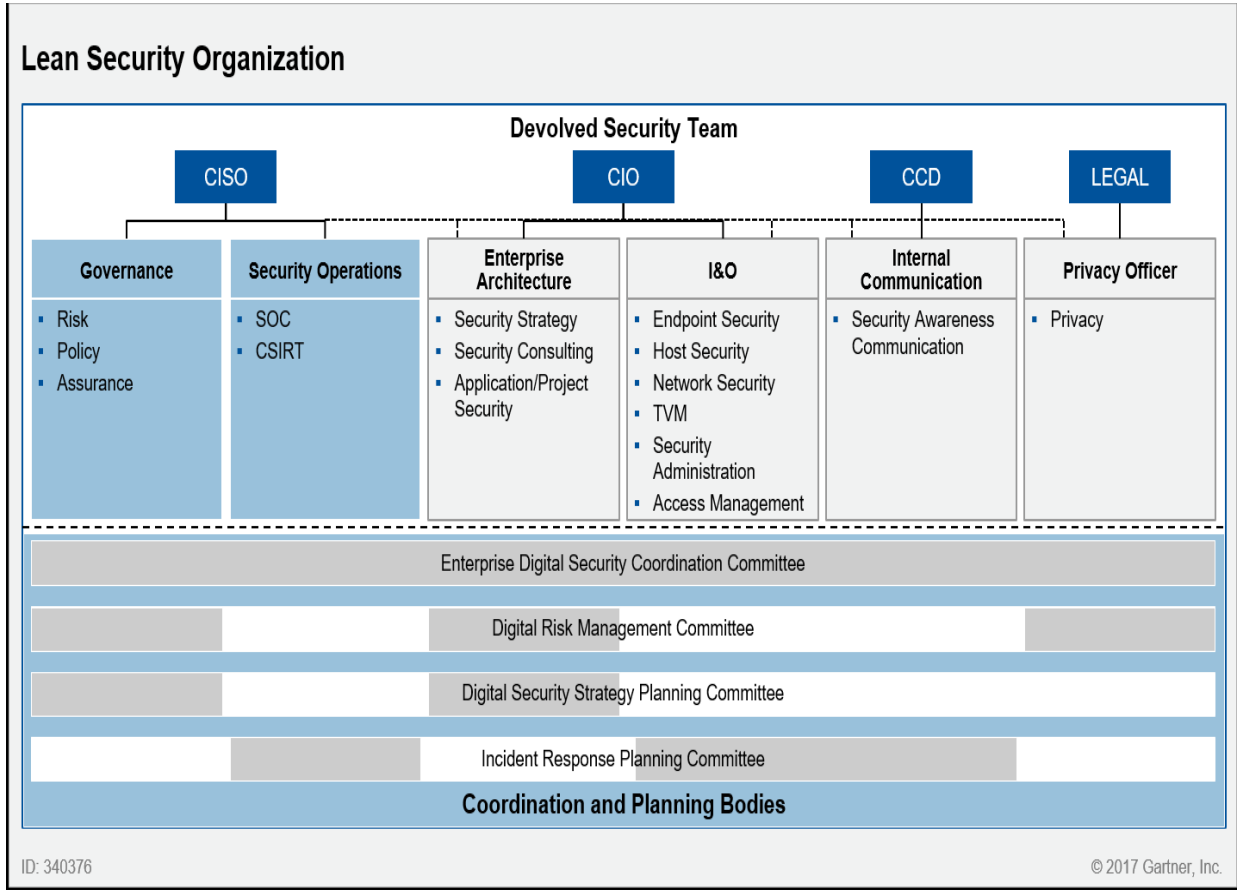
Most security leaders still believe that growing their dedicated security teams is an unavoidable consequence of digital risk

Table 1. Alternative Locations for Selected Security Functions

Security Function	Conventional Organizational Location	Potential Alternative Location
Program strategy/budget management	Information security (CISO) team	EA; IT strategy planning; PMO
Security process management	Information security (CISO) team	EA; I&O
Vendor/third-party/cloud security management	Information security (CISO) team	CIO (vendor relationship management); ITRM
Awareness communication	Information security (CISO) team	Communications department
Business continuity management	Information security (CISO) team	EA; ERM; DRM
Endpoint security	IT security	I&O — endpoint management
Host/server security	IT security	I&O — server management
Network security	IT security	I&O — network operations
Social and collaboration security	IT security	I&O — collaboration
Data security	IT security	Information management
Application security	IT security	Application development; DevSecOps teams
Identity intelligence/analytics	IT security	Other IAM functions; business intelligence and data analytics; internal audit

CISO: chief information security officer; DRM: disaster recovery management; EA: enterprise architecture; ERM: enterprise risk management; I&O: infrastructure and operations; IAM: identity and access management; ITRM: IT risk management; PMO: program management office

Source: Gartner (December 2017)



While Gartner research indicates that many security functions can effectively be "delegated" to other corporate, business and IT teams, such an approach is still anathema to many CISOs

Gartner

5

Machine Learning and AI

By 2025, it is expected that Machine Learning for aspects of security will be a normal part of security practices and will start to offset some skills and staffing shortfalls

***Artificial Intelligence (AI)** is technology that appears to emulate human performance typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogues with people, enhancing human cognitive performance or replacing people on execution of non-routine tasks. Applications include autonomous vehicles, automatic speech recognition and generation, and detecting novel concepts and abstractions - useful for detecting potential new risks and aiding humans to quickly understand very large bodies of ever-changing information.*

In its current state, ML/AI:

- is better at addressing *narrow and well-defined problem* sets (such as classifying executable files)
- provides the best value when it is *interpreted by humans*, or when it enhances operator awareness by providing relevant information
- helps short-staffed teams *be more efficient*, find threats they couldn't before, perform investigations more efficiently, and better anticipate future threats and risks
- is not, and *will never be, perfect*. It is trained, tuned and refined continuously by humans, and often incorporates the biases and preconceptions of programmers, which means it can be gamed

***Machine Learning (ML)** is a technical discipline to solve business problems utilizing mathematical models that can extract knowledge from data, in contrast to traditional software engineering which solves business problems by explicitly defining software logic. Mathematically, ML can solve a variety of problems related to search or optimization. ML approaches can heuristically search for a "best-fit" function, such that the function hopefully also performs well in new situations. The most common business functions supported by data science teams applying ML are marketing, strategic or financial planning, sales and risk, fraud, and compliance. However, the range of business problems that can be addressed with machine learning is huge.*

AI and ML are overloaded marketing terms, making it difficult to distinguish between hyperbole and genuine value. Applying ML well enough so that it can actually detect something new and unexpected is very difficult.

Gartner

The Promise of ML & AI

We can't escape the fact that humans and machines complement each other and together they can outperform each alone.

Lofty goals for incorporating ML/AI:

- Provides a verdict or decision with a high degree of confidence, allowing for credible decision support to improve the efficiency of security teams
- Provides transparency about the confidence level of the algorithms involved
- Uses training data that can help build an accurate representation of real-world security problems for supervised learning models
- Has good feature identification for unsupervised learning models
- Does not need frequent updates to the learning/analytics algorithms and/or does not need extensive manual rule writing/tuning
- Gets better over time, requiring progressively less human supervision
- Gives significantly better results than existing techniques

- Organizations are looking to ML/AI to help with the increased complexity of security data as well as to address staff shortages
- AI in security is being experimented with in many segments including application security, network security, data classification and data loss prevention, fraud detection, threat intelligence, security operations and integrated risk management (IRM)

Some of the early areas where AI technologies have been used successfully in security are:

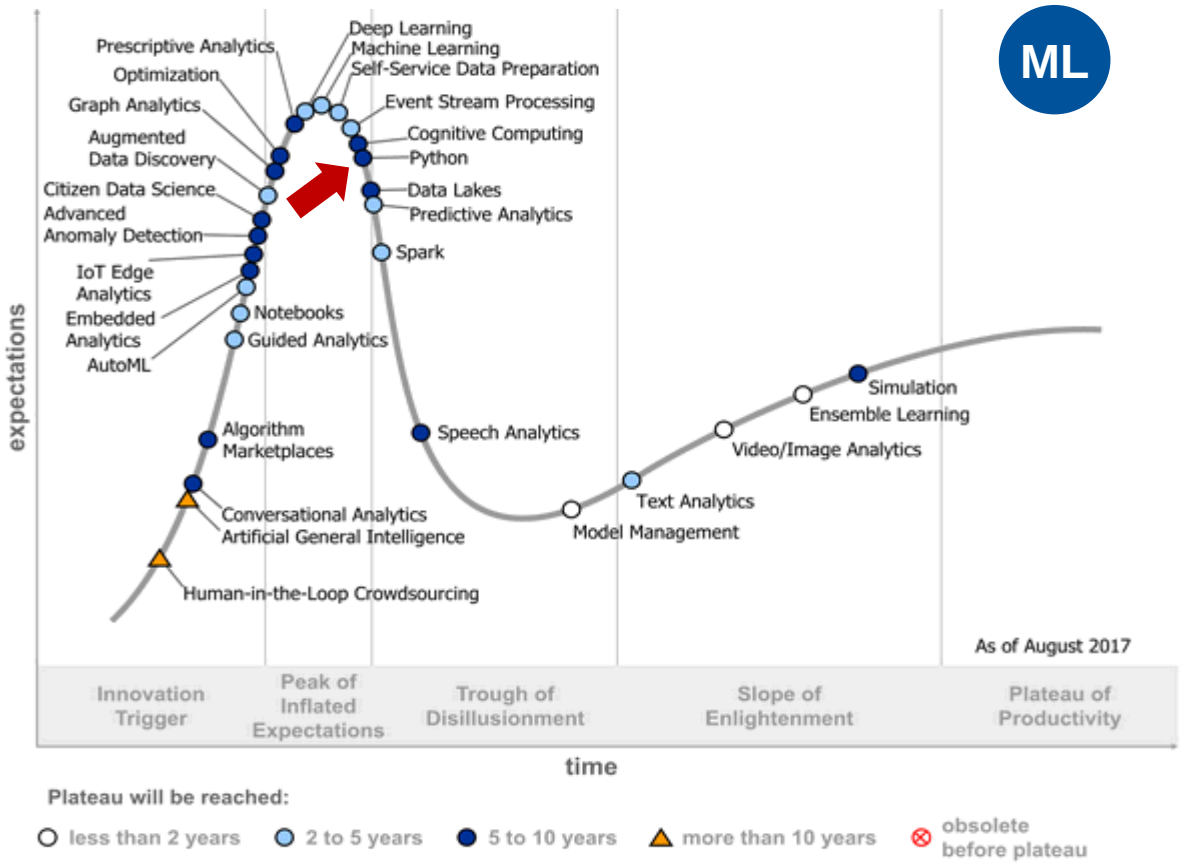
- *Threat Detection*: User and Entity Behavior Analysis
- *Decision Support*: Taking a variety of input and using analytics to suggest ways to speed up security processes
- *Vulnerability Management*: Applying threat intelligence and advanced analytics to existing vulnerability telemetry in order to enable a more accurate picture

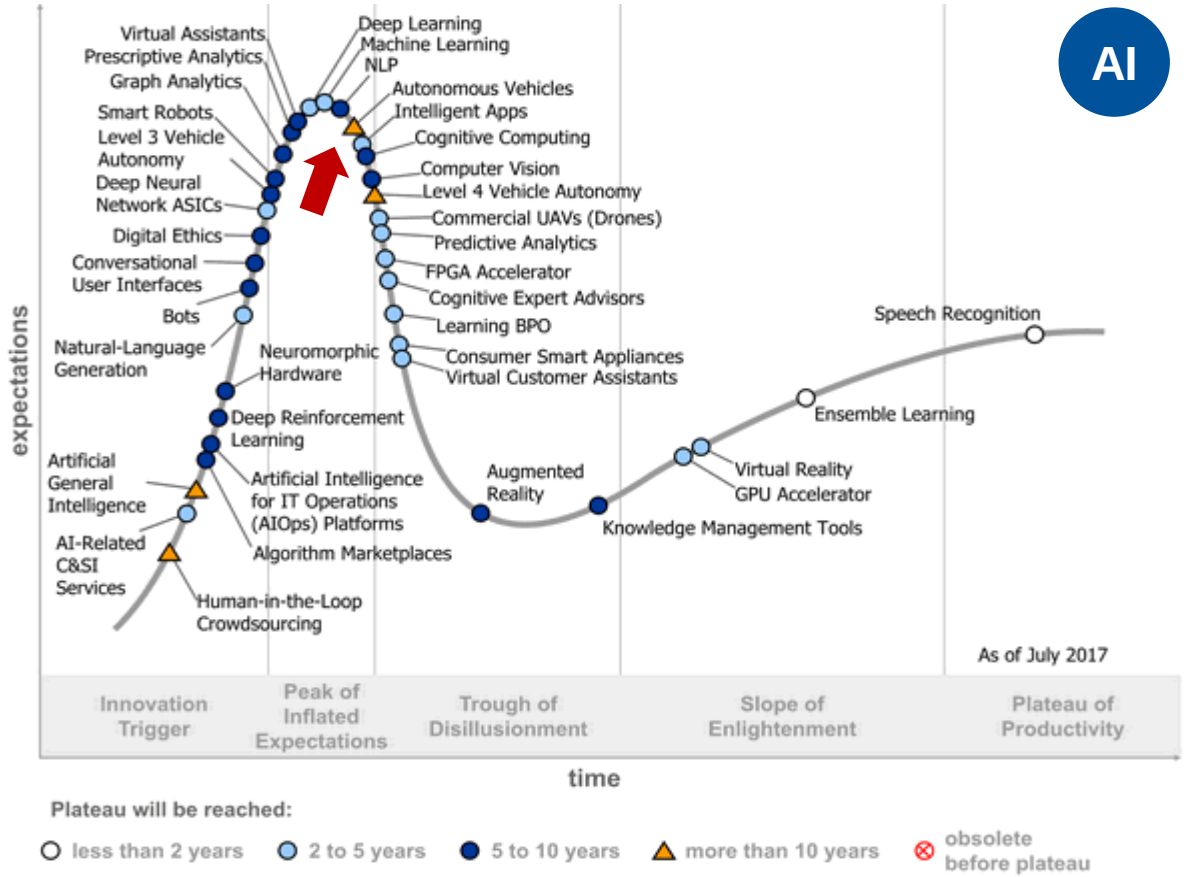
Enterprises are interested in AI-related approaches in security because they are curious whether such approaches can solve well-understood security and risk management challenges such as better prevention, improved detection, and faster incident response

Gartner

The Hype of ML & AI

The hype around these technologies has increased awareness and interest. But at the same time, it has heightened the confusion associated with their effective utilization.





ML and AI initiatives require more than just data and algorithms to be successful; they need a blend of skills, infrastructure and business buy-in.

Gartner

6

Changing the Paradigm

Security is a not a technology problem, but a people problem. It is people who develop the technology, manifest the threat and exploit the vulnerabilities, and develop and deploy remediation. But how we acquire and use human capital will change.

We must rethink our view of where to source sufficient numbers to do the things for which we cannot find alternatives

- Students
- Part-timers/2nd jobs
- New civilian veterans
- Sun-seeker/retirees
- Under-utilized population segments
- Partnerships with military, law enforcement, industry

More importantly, we must rethink our outlook for how these resources will be best engaged to contribute to our mission

The organization of the future will have few employees for the long-term. Think "time-slicing" or "time-sharing":

- By the semester or school year for students
- A few days per week/hours per day for part-timers
- By the season for retirees
- For a year or less for those in transition between job and career or changes in career

Most importantly, we must understand and execute what is necessary to make the change

- Deconstructing the Unicorn will be paramount in shifting the paradigm and making effective use of the new workforce within their requirements
- In the long run, benefits such as work-life balance, work place/time flexibility, and training & education will out-distance large pay differentials

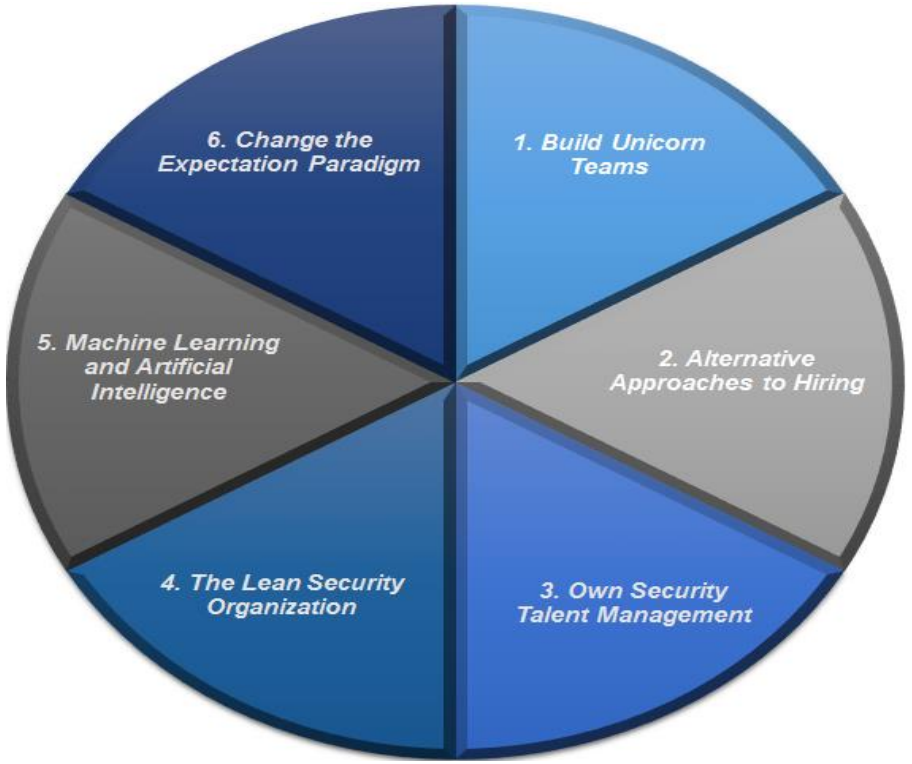
In the same way that people can be perceived as a workforce challenge, they also represent an incredible opportunity. New entrants to the workforce from both old and previously untapped sources bring a mix of enthusiasm and tested experience. Combined with a world-class educational system, we have the ability to create an unparalleled corps of new-era cybersecurity professionals.

Gartner

Wrap-Up & Q&A

Small security teams may not be hiring, but they are at the greatest risk of attrition, so they must improve staff development and engagement.

We are already struggling to hire and retain the right people. Growing team size and the emergence of new roles mean that Security can no longer take an impromptu, gut-driven approach to talent management.



The concept of security is simple. But executing security is a journey for which there are no shortcuts. It changes often and is no longer simply about technology. It's expensive and requires continuous investment. It takes time and requires constant attention and evolution. It forms complex relationships and is part of everything you do. And the need for it never ends. Endeavor to persevere.

Gartner

Additional Information Available

Recommended Gartner Research

- Build Security's Strategic Workforce Plan for the Digital Era
- Recruit Security Staff for the Digital Era
- Develop Existing Security Staff to Excel in the Digital Era
- Building the High-Performance Information Security Team

Texas DIR Information Security Forum

Gartner